Oracle Financial Services Enterprise Case Management: **Installation Guide - Stage 3**

Release 6.1
April 2012

ORACLE

Oracle Financial Services Enterprise Case Management: **Installation Guide - Stage 3**

Release 6.1
April 2012

Document Control Number: 9MN11-0009
Document Number: IG-11-OFS-0009-6.1-02-Stage 3

Oracle Financial Services Software, Inc.
1900 Oracle Way
Reston, VA 20190

Document Number: IG-11-OFS-0009-6.1-02-Stage 3
Second Edition (April 2012)

Copyright © 1996-2012, Oracle and/or its affiliates. All rights reserved.
Printed in U.S.A. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior written permission.

Trademarks
Oracle is a registered trademark of Oracle Corporation and/or its affiliates.
Other names may be trademarks of their respective owners.

Oracle Financial Services Software, Inc.
1900 Oracle Way
Reston, VA 20190
Phone: (703)-478-9000
Fax: (703)-318-6340
Internet: www.oracle.com/financialservices

Contents

List of Figures ..... ***vii***

List of Tables ..... ***ix***

About this Guide ..... ***xi***

Who Should Use this Guide xi
Scope of this Guide xi
How this Guide is Organized xii
Where to Find More Information xiii
Conventions Used in this Guide xiv

CHAPTER 1 ***Preparing to Install*** 1

Environment 1
Prerequisites 2
Pre-Installation Activities 2
Pre-Installation Checklist 3

CHAPTER 2 ***Installation Activities*** 5

Creating Atomic Schema Users 5
Configuring the log4j.xml 6
Permissible Values of the Attribute: 6
Populating the GRC_InstallConfig.xml File 7
Layer - GENERAL 8
Layer - APPLICATION 11
Layer - DATABASE 12
Layer - WEB 15
Installing Enterprise Case Management in Silent Mode 17

CHAPTER 3 ***Post Installation*** 19

Web Layer 19
For Websphere: 20
For Weblogic: 20
For Tomcat: 21

CHAPTER 4 ***Setting up Oracle Financial Services Enterprise Case Management Analytic Reports and Threshold Analyzer*** 23

Installing OBIEE Server 23
Post Installation Steps 23
Deploying Analytic Reports 24

CHAPTER 5 ***Deploying Network Visualization and Analysis*** 29

Prerequisites 29
Deploying Utility 30
Removing Existing Installation 30
Installing NetViz from New Installation Directory 31
Configuring Network Visualization and Analysis 31
Performing Application Server Configuration Tasks 31
Performing Network Manager Component Configuration Tasks 32
Performing Altio Presentation Server Configuration Tasks 32
Configuring Websphere Server to Support the PNG MIME Type 34
Managing Cookies in WebLogic 10.3.1 35
Configuring WebLogic Application Server to support the PNG MIME type 36

APPENDIX A ***About OBIEE 37***

Creating ODBC Connection 37
Configuring OBIEE Connection Pool 42
Configuring OBIEE Dashboard Access Control 46

APPENDIX B ***Installing and Configuring Altio Server 51***

Installing Altio Presentation Server 51
Accessing Altio Presentation Server Console 52
Configuring Altio Presentation Server 53

APPENDIX C ***Installation of Oracle Financial Services Enterprise Case Management Active Pages 55***

Extracting Oracle Financial Services Active Pages 55

List of Figures

Figure 1. Business Intelligence Core Application page 25
Figure 2. Application Lock and Edit Configuration page 26
Figure 3. IFrame Tag Details 28
Figure 4. Run Dialog Box 37
Figure 5. ODBC Data Source Administrator Dialog Box 38
Figure 6. Create New Data Source Dialog Box 39
Figure 7. Oracle BI Server DSN Configuration Dialog Box 40
Figure 8. Oracle BI Server DSN Configuration Login Dialog Box 41
Figure 9. Oracle BI Administration Tool 42
Figure 10. Open Online Dialog Box 43
Figure 11. Oracle BI Administration Tool - MantasBI_Merged.rpd 44
Figure 12. Connection Pool Dialog Box 45
Figure 13. Oracle Business Intelligence Login Page 46
Figure 14. OBIEE Dashboard Page 47
Figure 15. Manage Catalog Group page 48
Figure 16. Manage Catalog Group Names page 49
Figure 17. Edit Group page 50

List of Tables

Table 1. Conventions Used in this Guide xiv
Table 2. Environment Details 1
Table 3. Pre-Installation Checklist 3
Table 4. Interaction Groups in Layer - GENERAL 8
Table 5. Interaction Groups in Layer - APPLICATION 11
Table 6. Interaction Groups in Layer-DATABASE 12
Table 7. Interaction Groups in Layer - WEB 15
Table 8. Parameters for the Properties Tag in the altioapp.xml File 33

About this Guide

This guide provides comprehensive instructions for installing and configuring the Oracle Financial Services Enterprise Case Management, Release 6.1 (herein referred to as OFS ECM), and associated solution sets.

This chapter focuses on the following topics:

- Who Should Use this Guide
- Scope of this Guide
- How this Guide is Organized
- Where to Find More Information
- Conventions Used in this Guide

Who Should Use this Guide

The *Oracle Financial Services Enterprise Case Management Installation Guide - Stage 3* is designed for use by the OFS ECM Installers and System Administrators. Their roles and responsibilities include the following:

- **OFS ECM Installer:** This user installs and configures the Enterprise Case Management solution at the deployment site.
- **System Administrator:** This user installs, configures, maintains, and adjusts the system and is usually an employee of a specific Enterprise Case Management client. The System Administrator maintains user accounts and maps roles to users.

Scope of this Guide

This guide provides step-by-step instructions for installing the OFS ECM Solution on an existing Oracle Financial Services Analytical Applications Infrastructure (OFSAAI).

How this Guide is Organized

The *Oracle Financial Services Enterprise Case Management Installation Guide - Stage 3* includes the following chapters:

- Chapter 1, *Preparing to Install,* details the activities that occur prior to the deployment, typical installation configuration, and identifies all third-party software necessary to run the application.
- *Chapter 2, Installation Activities,* provides step-by-step installation activities for installing the OFS ECM.
- Chapter 3, *Post Installation,* details the steps that are required to be performed after successful installation of OFS ECM.
- Chapter 4, *Setting up Oracle Financial Services Enterprise Case Management Analytic Reports and Threshold Analyzer,* explains how to apply and display Analytic Reports and Threshold Analyzer in the OFS ECM UI.
- Chapter 5, *Deploying Network Visualization and Analysis,* details the process of deploying the Network Visualization and Analysis utility to an existing Altio environment. Also details the steps that are required to be performed after installing OFS ECM successfully.
- Appendix A, *About OBIEE,* explains the OBIEE Connection Pool Configuration, details the configuration steps for the OBIEE Connection Pool.
- Appendix B, *Installing and Configuring Altio Server,* details the steps for installing and configuring the Altio Server.
- Appendix C, *Installation of Oracle Financial Services Enterprise Case Management Active Pages,* details the installation process of the Oracle Financial Services Active Pages.

Where to Find More Information

The OFS ECM installation is done in three stages. This guide is Stage 3 manual. The names of three installation guides are listed below:

- (Stage 1) *Oracle Financial Services Behavior Detection Platform Installation Guide Stage-1:* This manual provides instructions for installing Oracle Financial Services scenarios and data ingestion algorithms to support behavior detection.
- (Stage 2) *Oracle Financial Services Analytical Applications Infrastructure Installation and Configuration Release 7.3:* This manual details the steps involved in installing OFSAAI in the released environment.
- (Stage 3) *Oracle Financial Services Enterprise Case Management Installation Guide Stage- 3:* This guide provides comprehensive instructions for installing and configuring OFS ECM and the associated solution set.

For more information about OFS ECM, refer to the following documents:

- *Oracle Financial Services Behavior Detection Platform Configuration Guide:* Provides instruction on how to configure the Oracle Financial Services application User Interface.
- *Oracle Financial Services Analytical Applications Infrastructure Installation and Configuration Release 7.3*: Provides step-by-step instructions necessary for configuring Oracle Financial Services Analytical Applications Infrastructure.
- *Oracle Financial Services Analytical Applications Infrastructure User Manual Release 7.3* This manual deals with the System Configuration and Administration components of Infrastructure and assists the administrator in configuring the system, managing the users, and performing administrative tasks effectively.

To find additional information about how OFS ECM solves real business problems, see our website www.oracle.com/financial services.

Conventions Used in this Guide

Table 1 lists the conventions used in this guide.

Table 1. Conventions Used in this Guide

This convention. . .	Stands for . . .
Italics	• Names of books, chapters, and sections as references • Emphasis
Bold	• Object of an action (menu names, field names, options, button names) in a step-by-step procedure • Commands typed at a prompt • User input
`Monospace`	• Directories and subdirectories • File names and extensions • Process names • Code sample, including keywords and variables within text and as separate paragraphs, and user-defined program elements within text
<Variable>	Substitute input value

CHAPTER 1 Preparing to Install

This chapter provides information about system hardware and software requirements and pre-installation activities.

This chapter includes the following topics:

- Environment
- Prerequisites
- Pre-Installation Activities
- Pre-Installation Checklist

Environment

Table 2. Environment Details

Back- End Environment	Hardware	Software
RHEL 5.3 /5.5 or Sun Solaris 10 - 64 Bit	64-bit x 86 architecture	• Oracle 11g R2 (11.2.0.1.0) - 64 bit • Java 1.6 -64 bit • Websphere 7.0.0.21 -64 bit or Weblogic 10.3.5 – 64 bit • Oracle Behavior Detection platform 6.1 • OBIEE 11.1.1.6 • Altio 5.1.5 • NetViz 1.2.7e • OFSAAI 7.3
Front-End Client Access		**Software**
		• Java Plug-in 1.6.0_18 • Client Machines -Download: Windows XP Service Pack 3 • Microsoft Internet Explorer 7.0 and 8.0 • Microsoft Excel 2003 • Adobe Reader 8.0 • Supported Screen Resolutions- 1024*768 and 1280*1024

Prerequisites

- Oracle Financial Services Behavior Detection must be installed and configured. Refer to *Oracle Financial Services Behavior Detection Platform Installation Guide Stage -1*, for more information.
- Oracle Financial Services Analytical Applications Infrastructure (OFSAAI) must be installed and configured with server details. For assistance in configuring the OFSAAI platform, refer to the *Oracle Financial Services Analytical Applications Infrastructure Installation and Configuration Release 7.3* , for more information.

  Note: Infodom and Segment creation, and their mapping is done by the Installer.

Pre-Installation Activities

This section explains the pre-installation activities to be performed by the OFS ECM System Administrator.

Before installing OFS ECM, perform following pre-installation activities:

1. Take the back up of the following:
   - `Infrastructure Configuration Schema`
   - `Infrastructure Installation directory`
   - `Alert Management Schema`
   - `Case Management Schema`
   - `Business and Market Schemas`

   Note: The backup must be kept until the successful installation of the application.
2. Extract the following files from the media pack to a folder on the machine that hosts the OFSAAI platform:

   Note: The folder and files must have Execute permission.
   - `Setup.bin`
   - `Setup.sh`
   - `GRC_InstallConfig.xml`
   - `validateXMLInputs.jar`
   - `log4j.xml`
   - `CreateAtomicUser.jar`

   Note: `Setup.bin`,`CreateAtomicUser.jar and validateXMLInputs.jar` should be extracted in binary mode. `Setup.sh` and `GRC_InstallConfig.xml` should be extracted in text mode.

Pre-Installation Checklist

Table 3 lists the pre-installation activities that need to be completed before starting the installation of OFS ECM.

Table 3. Pre-Installation Checklist

Step No.	Task	Done
1	Ensure that the system hardware and software are available as mentioned in the *Prerequisites*, on page 2.	☐
2	Ensure that the Oracle Financial Services Behavior Detection platform is installed and configured.	☐
3	Ensure that the OFSAAI 7.3 is installed and configured with server details.	☐
4	Ensure that the Oracle Database is up and running, and the following schemas are available: • `Alert Management Schema` • `Infrastructure configuration schema` • `Case Management Schema` • `Configuration Schema` • `KDD ALG Schema` • `KDD MNR Schema` • `KDD Web Schema` • `KDD Schema` • `KDD Altio Schema` • `DB UTIL Schema` **Note:** You must have a valid User ID and Password for each schema. A separate utility has been included along with Installation files to create Alert Management Schema and Case Management Schema. Refer to *Chapter 2, Installation Activities,* for more information.	☐
5	Ensure that Application servers are up and running while Installing the App Layer.	☐
6	Ensure that the Oracle database instance is up and running.	☐
7	Ensure that the `FTPshare` path is configured and available in the OFSAAI Platform.	☐
8	Ensure that the IP addresses or host names of the OFSAAI App and Web Layer are available.	☐
9	Ensure that the Servlet port is available.	☐
10	Ensure that the `ftpshare` path of the OFSAAI Application Layer (APP), Data Base Layer (DB) and Web Application Layer (WEB) layers have Recursive Write permission.	☐
11	Ensure that `Setup.bin`, `Setup.sh`, `validateXMLinputs.jar`, `log4j.xml`, `CreateAtomicUser.jar` and `GRCInstall_Config.xml` files are copied to the machine that hosts the OFSAAI platform and has the necessary permissions.	☐
12	Ensure that the database instance parameter processes is set to a minimum value of 500.	☐

Table 3. Pre-Installation Checklist

Step No.	Task	Done
13	Check whether the `Reveleus.SEC` is present in `<OFSAAI_DB_LAYER>/conf` (In case of Multi-tier installation). If it is not present, copy `Reveleus.SEC` file from `<OFSAAI_APP_LAYER>/conf` and paste it in `<OFSAAI_DB_LAYER>/conf`. **Note:** This step is applicable only for multi-tier installation.	☐
14	Ensure that you have sufficient temp space (1 GB) for your installation.	☐

CHAPTER 2 Installation Activities

This chapter describes the installation process in a multi-tier and single-tier environment in which the solution setup components are installed on separate machines.

This chapter covers the following topics:

- Creating Atomic Schema Users
- Configuring the log4j.xml
- Populating the GRC_InstallConfig.xml File
- Installing Enterprise Case Management in Silent Mode

OFS ECM comprises the components that are installed in the OFSAAI platform Web, Application, and Database layers. If OFSAAI has been installed in a multi-tier architecture, then the installer must be invoked for each machine that hosts an OFSAAI tier.

Note: With multi-tier installations, you need to install APP-Layer first, then DB-Layer, and finally Web-Layer. During APP-Layer installation, the APP Server should be up and running.

Creating Atomic Schema Users

This section explains the steps to create Atomic Schema Users, if it has not been done as a part of Pre-Installation Activities. To perform this task, you require user name and password of a DB user with SYSDBA privileges.

To create Atomic Schema User, follow these steps:

1. On the machine, navigate to the directory where `CreateAtomicUser.jar` has been copied.
2. Execute the below command in SSH:

   ```
   java -jar  CreateAtomicUser.jar
   ```

3. Provide the parameters you are prompted to input. This will include Solution Name (ECM in this case), username and password of DB user with SYSDBA privileges and Atomic Schema User Names and Passwords.

Configuring the log4j.xml

This section explains the steps to configure the `log4j.xml` file which determines the output produced in the logs.

1. To set the path and name of the log file, edit the value of the *value* attribute in the corresponding *param* node as shown below.

   ```
   <param name="file" value="="/home/test73app/grckit/log.log"/>
   ```

2. To set the append mode, edit the value of *value* attribute in the corresponding *param* node as true/false.

   ```
   < param name="append" value="true"/>
   ```

3. To set the size of the log file, edit the value of *value* attribute in the corresponding *param* node as shown below.

   ```
   < param name="MaxFileSize" value="100000kb"/>
   ```

4. To change the information to be displayed in logs, edit the value of *value* attribute in *priority* node as shown below.

   ```
   < priority value="debug"></priority>
   ```

Permissible Values of the Attribute:

- **Debug**- it displays the values of different variables along with the content displayed by info, warn, and fatal.
- **Info**- it displays the flow of control of installer along with the cotent displayed by warn and fatal.
- **Warn**- it displays all the exceptions occurred during installation along with the content displayed by fatal.
- **Fatal**- it displays all the errors occurred during installation.

Populating the GRC_InstallConfig.xml File

This section explains the steps to populate the `GRC_InstallConfig.xml` file.

To populate `GRC_InstallConfig.xml`, follow these steps:

1. Open the existing `GRC_InstallConfig.xml` under OFS ECM installer kit directory and enter the required input parameters as per the instructions below.
2. Copy the populated `GRC_InstallConfig.xml` to OFS ECM installer kit directory before proceeding with OFS ECM installations.

   This file contains the following four layers:

   - GENERAL
   - APPLICATION
   - DATABASE
   - WEB

Layers are divided into different Interaction Groups. The Interaction Group defines the type of Interaction Variables. These Variables contain Interaction Parameters required for the installation of Infrastructure.

Note: Interaction Variables value can not be Null, retain NA for any variable that is not applicable for the installation. For all the installation layers, GENERAL layer info is mandatory.

Layer - GENERAL

The Layer GENERAL (`<Layer name="GENERAL">`) contains the following nodes to provide the parameter values for the below mentioned Interaction Groups:

Table 4. Interaction Groups in Layer - GENERAL

Interaction Group Name	Details of the Values to be Assigned to the Interaction Group

OFSAAI Customer Code	This node is for installing the Customer Code.
	
	Following is the code for this node:
	
	`<Interaction Group name="OFSAA Infrastructure Customer Code">`
	`<InteractionVariable name="CUSTID">EDELIVERY</InteractionVariable>`
	`</InteractionGroup>`
	Note: This node cannot be left NA if the installation is done in the Silent mode. EDELIVERY is the hard-coded value for this tag.

Choose OFSAAI Layer	This node is for the Installation Mode. Permissible values for each Interaction variable are `0` and `1`. This can be Single-Tier or Multi-Tier.
	
	`<InteractionGroup name="Choose OFSAAI Layer">`
	`<InteractionVariable name="APP_LAYER">0</InteractionVariable>`
	`<InteractionVariable name="DB_LAYER">1</InteractionVariable>`
	`<InteractionVariable name="WEB_LAYER">0</InteractionVariable>`
	`</InteractionGroup>`
	
	Note: If you enter all three fields `APP_LAYER`, `DB_LAYER`, and `WEB_LAYER` as `1`, then it is Single-Tier installation.
	For example, if you are installing DB and WEB on the same machine, then you must put `InteractionVariable name="DB_LAYER"=1`, `InteractionVariable name="WEB_LAYER"=1`, and `InteractionVariable name="APP_LAYER"=0`

Table 4. Interaction Groups in Layer - GENERAL (Continued)

Interaction Group Name	Details of the Values to be Assigned to the Interaction Group

Pre-Installation Details	If you want Pre-Installation steps to be automated, this node should have the value `1` in App Layer. For other layers, it should have the value `0`.
	
	`<InteractionGroup name="PRE-INSTALLATION">`
	`<InteractionVariable`
	`name="PRE_INSTALL">1</InteractionVariable>`
	`</InteractionGroup>`
	
	The value of this node cannot be NA. Permissible values for this node are `0` and `1`.
	● `1` If the Pre-Installation steps like Infodom Creation,Model Upload,ETL Sources creation are to be automated
	● `0` If the user has furnished the above details through front-end.
	
	Note: If the Pre-Installation node is given the value `1`, then the default OFSAAI user for ETL source creation and Data model upload is SYSADM. The OFSAAI server must be started prior to the solution Installation in APP layer.

Table 4. Interaction Groups in Layer - GENERAL (Continued)

Interaction Group Name	Details of the Values to be Assigned to the Interaction Group

Installation Details	For OFS ECM 6.1 installation, all the fields under this parameter are to be completed.
	
	`<InteractionGroup name="Installation Details">`
	`<InteractionVariable name="INFODOM_NAME">AMINFO</InteractionVariable>`
	`<InteractionVariable name="SEGMENT_CODE">AMSEG</InteractionVariable>`
	`<InteractionVariable name="INFODOM_NAME_2">CMINFO</InteractionVariable>`
	`<InteractionVariable name="SEGMENT_CODE_2">CMSEG</InteractionVariable>`
	`<InteractionVariable name="LOCAL_FTPSHARE_PATH">/d01/grcapp/ftpshare</InteractionVariable>`
	`</InteractionGroup>`
	
	Tags and names:
	
	● `INFODOM_NAME`: Name of the Infodom
	● `SEGMENT_CODE`: Name of the Segment
	● `INFODOM_NAME_2`: Name of Second Infodom, if it is required by the application.
	● `SEGMENT_CODE`: Name of the Second Segment, if it is required by the application.
	● `LOCAL_FTPSHARE_PATH`: Enter the local Ftpshare path of the layer (APP, DB, or WEB) in which you are installing.
	
	Suppose you are doing installation in APP Layer then you have to enter `/home/grcapp/ftpshare.`
	
	Note: For OFS ECM 6.1, you must enter the value of Alert Management Infodomand Segment under `INFODOM_NAME` and `SEGMENT_CODE` respectively.
	Under `INFODOM_NAME_2` and `SEGMENT_CODE_2`, you must enter the value of Case Management Infodom and Segment details.

Layer - APPLICATION

The variables under this layer consist of the following nodes, which must be configured for installation of Application Layer as one of its component.

Table 5. Interaction Groups in Layer - APPLICATION

Interaction Group Name	Details of the Values to be Assigned to the Interaction Group

Pre-Installation Configuration	The following is the code for this node:
	
	`<InteractionVariable name="INFODOM_FLAG">1</InteractionVariable>`
	`<InteractionVariable name="INFODOM_COUNT">2</InteractionVariable>`
	`<InteractionVariable name="DATAMODEL_FLAG">0</InteractionVariable>`
	`<InteractionVariable name="DATAMODEL_TYPE">0</InteractionVariable>`
	`<InteractionVariable name="DM_FILE_NAME">NA</InteractionVariable>`
	`<InteractionVariable name="DATAMODEL_PATH">NA</InteractionVariable>`
	`<InteractionVariable name="ETL_CREATION">0</InteractionVariable>`
	
	Tag name and values:
	
	● INFODOM_FLAG: Permissible value is either `0` or `1`. If this node is given the value `1`, then the infodom creation will be through Installer else in case of `0`,Infodom should be created before ECM 6.1 installation.
	● INFODOM_COUNT: This field specifies how many Infodoms does the user want. If `1` is entered, `1` infodom will be created. Similiarly, if `2` is entered, `2` infodoms are created.
	● DATAMODEL_FLAG: Keep this value as `0` for ECM.
	● DATAMODEL_TYPE: Keep this value as `0` for ECM.
	● DM_FILE_NAME:Keep this value NA.
	● DATAMODEL_PATH: Keep this value NA.
	● ETL_CREATION: Keep this value as `0` for ECM.

Layer - DATABASE

The variables under this layer consist of the following nodes, which must be configured for installation of Database Layer as one of its component.

Table 6. Interaction Groups in Layer-DATABASE

Interaction Group Name	Details of the Values to be Assigned to the Interaction Group
Database Details	Specify the Config Schema URL and driver for the connection purpose. This node allows you to specify the database details needed for the database connection. The following is the code for this node: `<InteractionGroup name="Database Details" > <InteractionVariable name="DATABASE_URL">jdbc:oracle:thin:@10.184.62.180:1522:orcl10gr</InteractionVariable> <InteractionVariable name="FICMASTER_DRIVER">oracle.jdbc.driver.OracleDriver</InteractionVariable> </InteractionGroup>` The value of both the parameters are available in the file- `DynamicServices.xml` under `<APP_HOME>/conf` **Note:** Value cannot be Null for these parameters.

Table 6. Interaction Groups in Layer-DATABASE (Continued)

Interaction Group Name	Details of the Values to be Assigned to the Interaction Group
OFS ECM Schema Details	Specifies the schemas used in the installation and Tablespace (as applicable). Usernames of the other OFS ECM schemas are to be entered in this section. The following is the code for this node: InteractionGroup name="FS ECM Schema Details" > <InteractionVariable name="BUSINESS_SCHEMA_USER">bususer</InteractionVariable> <InteractionVariable name="MANTAS_SCHEMA_USER">amuser</InteractionVariable> <InteractionVariable name="MARKET_SCHEMA_USER">maruser</InteractionVariable> <InteractionVariable name="KDD_WEB_SCHEMA_USER">kdd_web</InteractionVariable> <InteractionVariable name="KDD_SCHEMA_USER">kdduser</InteractionVariable> <InteractionVariable name="KDD_MNR_SCHEMA_USER">kddmnruser</InteractionVariable> <InteractionVariable name="DB_UTIL_USER">kdduser</InteractionVariable> <InteractionVariable name="KDD_ALG_SCHEMA_USER">kddalguser</InteractionVariable> <InteractionVariable name="KDD_ALTIO_USER">kddaltiouser</InteractionVariable> <InteractionVariable name="KDD_ALGORITHM">kddalgorithm</InteractionVariable> <InteractionVariable name="KDD_ANALYST">kddanalyst</InteractionVariable> <InteractionVariable name="TABLE_SPACE">NA</InteractionVariable> </InteractionGroup> **Note:** "KDD_ALGORITHM and "KDD_ANALYST" are roles. • All the parameters are necessary and <InteractionVariable name="TABLE_SPACE"> is not required. • KDD_ALGORITHM and KDD_ANALYST roles should be mentioned in the <InteractionVariable name="KDD_ALGORITHM"> and <InteractionVariable name="KDD_ANALYST"> respectively. **Note:** TABLE_SPACE value for the OFS ECM installation must be NA.

Table 6. Interaction Groups in Layer-DATABASE (Continued)

Interaction Group Name	Details of the Values to be Assigned to the Interaction Group
OFS ECM AdminTools - Context Root Name	This field takes the context name for the Admin Tools for deployment purpose. Following is the code for this node: `<InteractionGroup name="FS ECM AdminTools- Context Root Name" > <InteractionVariable name="ADMIN_CONTEXT_NAME">admin_tools</InteractionVariable> </InteractionGroup> </Layer>` **Note:** The value of the above variable cannot be Null or NA for the OFS ECM installation.

Layer - WEB

The variables under this layer consist of following nodes which must be configured for installations of the WEB layer as one of its component:

Table 7. Interaction Groups in Layer - WEB

Interaction Group Name	Details of the Values to be Assigned to Interaction Group
Database Details	For the tag FICMASTER_USER, you have to enter the value of OFSAAI Configuration Schema user. Following is the value of node under this group. `<InteractionVariable name="FICMASTER_USER">confuser</InteractionVariable> </InteractionGroup>` **Note:** This value cannot be NA.
OFS ECM Schema Details	Specifies the schemas used in the installation. User names of the other OFS ECM schemas (Business Schema, Market Schema, Mantas Schema, KDD-Web Schema, KDD Schema, and KDD-MNR Schema) are to be entered in this section. Following is the code for this node: `<InteractionGroup name="FS ECM Schema Details" > <InteractionVariable name="BUSINESS_SCHEMA_USER">NA</InteractionVariable> <InteractionVariable name="MARKET_SCHEMA_USER">NA</InteractionVariable> <InteractionVariable name="MANTAS_SCHEMA_USER">NA</InteractionVariable> <InteractionVariable name="KDD_WEB_SCHEMA_USER">NA</InteractionVariable> <InteractionVariable name="KDD_SCHEMA_USER">NA</InteractionVariable> <InteractionVariable name="KDD_MNR_SCHEMA_USER">NA</InteractionVariable> </InteractionGroup>.` **Note:** All parameters are necessary and are part of pre-installation check-list.

Table 7. Interaction Groups in Layer - WEB (Continued)

Interaction Group Name	Details of the Values to be Assigned to Interaction Group
OBIEE Reports Installation	This is to specify whether the Oracle Business Intelligence Enterprise Edition (OBIEE) needs to be integrated in the setup or not. Following is node under this group: `<InteractionGroup name="OBIEE Reports Installation" > <InteractionVariable name="OBIEE_REPORTS">1</InteractionVariable> </InteractionGroup> </Layer>` **Note:** For the tag `OBIEE_REPORTS`, only values `1` or `0` can be entered. • `1` to install the `OBIEE reports` • `0` not to install the `OBIEE reports`

Installing Enterprise Case Management in Silent Mode

This section explains the steps to install the OFS ECM 6.1 in Silent Mode.

To install OFS ECM in Silent Mode, follow these steps:

1. On the machine, navigate to the directory where `Setup.sh` has been copied.
2. Execute the below command in `SSH:`

   ```
   ./Setup.sh SILENT
   ```

   Note: In Silent Mode of OFS ECM Installation, you will be prompted for parameters like `OFSAAI Schema Password, Alert Management Schema Password, KDD_Web Schema Password, KDD_MNR Schema Password, KDD Schema Password, Business Schema Password, Market Schema Password,` and `KDD_Altio Schema Password` in the command prompt (Passwords will be masked).
3. Provide the necessary parameters and proceed with the installation.
4. Once you comple installation, then check the installation logs for any errors.
5. The installation process generates log files in the Infrastructure Installation directory. Two logs - `Path as per log4j.xml e.g., /home/test73app/grckit/long.log` and `SolutionSetup_InstallLog.log` will be created.

   Note: The log `AMCM_SolutionLog_timestamp.log` provides the status of execution of scripts, updates `ETL Repository.xml` and `web.xml`, and so forth. The log `SolutionSetup_InstallLog.log` provides the status of the installation of OFS ECM components.

   Note: If you observe any `Warnings/Non Fatal Errors/Fatal Errors/Exceptions` reported in either of the logs, bring them to the notice of the OFS ECM Support personnel. Do not proceed with the rest of the instructions until all such issues are adequately addressed.
6. Upon successful installation, proceed to post installation steps as explained in the next chapters.

CHAPTER 3 Post Installation

This chapter gives you complete information on the Post Installation activities.

Once the installation of the OFS ECM is completed, restart all the application servers and follow these steps:

Note: To start application servers, refer to the section *Starting Application Servers in Configuration of Resource Reference* in *Oracle Financial Services Analytical Applications Infrastructure Installation and Configuration Release 7.3*.

During the restart of OFSAAI application server, ignore the below message appearing on the console of OFSAAI application server and proceed further. (the placeholders `<AMINFODOM>` and `<CMINFODOM>` in the message are replaced with the Alert Management Infodom created).

```
"java.io.FileNotFoundException:
/software/fccm61t/fccm60ftp/fccm_61_demo_drive/ftpshare/<AMINFODOM>
/erwin/fipxml/<AMINFODOM>_DATABASE.XML (No such file or directory)"

"java.io.FileNotFoundException:
/software/fccm61t/fccm61ftp/fccm_61_demo_drive/ftpshare/<CMINFODOM>
/erwin/fipxml/<CMINFODOM>DATABASE.XML (No such file or directory)"
```

Web Layer

1. Login to the Web Application server console for creating Java Data Base Connectivity (JDBC) resources for Alert Management and Case Management. For more information, refer to the section *Configuration of Resource Reference* in *Oracle Financial Services Analytical Applications Infrastructure Installation and Configuration Release 7.3*.
2. Go to `< FIC_HOME >/AM` installed directory and run the script file `changePasswords.sh`
3. Go to `< FIC_HOME >/AM` installed directory and run the script file `create_at_war.sh`
4. Deploy the `<Context-name>.ear (for example, OFSAAI.ear)` available at `< FIC_HOME >/ficweb` directory.
5. Deploy the `<admin_tool_context-name>.war(that is, admin_tools.war)` available at `<OFSAAI_PROD_INSTALL_DIR>/AM` directory as an application on your Web Server.

   Note: Ensure that Security Attributes mapping is done before accessing Admin Tools application for privileged users/user groups and restart the admin tools applications.

   Note: For instructions on deploying the EAR file, refer to *Oracle Financial Services Analytical Applications Infrastructure Installation and Configuration Release 7.3*, for more information.

6. If the administration tool is deployed on a separate application server, then follow these steps:
   a. Login to Alert Management Atomic Schema.
   b. Run the query: `Update KDD_INSTALL_PARAM Set ATTR_2_VALUE_TX='##WEB_APP_SERVER_URL##' WHERE PARAM_ID=20`
   c. Replace the placeholder `(##WEB_APP_SERVER_URL##)` with appropriate value before running the above update.
7. Check and ensure that the placeholders (`PORT,CONTEXT`) were updated with appropriate values within `DynamicWsConfig.xml` located at `<<FIC_HOME>>/EXEWebservice/<<Web Application server>>/ROOT/conf`
8. To deploy `EXEWebService:`
   a. Navigate to `<FIC_HOME>/EXEWebService/<Webserver>` directory.
   b. Run the command:

      `./ant.sh`

      This will create `EXEWebService.ear` under same directory.
   c. Deploy `EXEWebService.ear` in Webserver.
9. Restart all application servers.
   a. Go to `<FIC_APP_HOME>/common/FICServer/bin` and run the file `reveleusstartup.sh`
   b. Start the Web Application server.
10. To check or modify the connection pool settings for Alert Management and Case Management datasources,follow these steps depending on the type of Web Application server (Websphere/Weblogic/Tomcat) used:

For Websphere:

   a. Login to Websphere admin console.
   b. Click on **Resources**, select **JDBC**, select **JDBC Providers**.
   c. Click on data sources applicable for ECM (Do the settings for both alert and case management data sources).
   d. In additional properties, click on **Data Sources**.
   e. Again click on data source name.
   f. In additional properties, click on **Connection Pool Properties**.

Note: If the value for the maximum connection is less than '50', then make it to 50.

For Weblogic:

   a. Login to Weblogic admin console.

b. Click on **Services**, select **JDBC,** select **Data Sources**.

c. Click on data sources applicable for ECM 6.1(Do the settings for both Alert Management and Case Management data sources).

d. Click on **Connection Pool** Tab.

Note: If the value for the maximum capacity is less than '50', then make it to 50.

For Tomcat:

a. Navigate to `<<Tomcat_Installation_Directory>>/conf/Server.xml` file.

b. Go to ECM 6.1 specific resource tags defined for Alert Management and Case Management Infodoms.

Note: If the maxActive value is less than '50', then make it to 50.

11. Steps to access the OFS ECM User Interface (UI):

    a. Log in as `sysadmn`, map the OFS ECM User Group to the role *Mantas Administrator*.

    b. Unmap Case Management information domain from the OFS ECM.

    Note: Refer to *Oracle Financial Services Analytical Applications Infrastructure User Manual Release 7.3* for more information.

    c. Login as OFS ECM Admin User with valid username and password, you are navigated to Home page, and then select Enterprise Case Management as default page and click **Save**.

    d. Re-login to the UI to access OFS ECM UI.

    Note: Refer to *Oracle Financial Services Enterprise Case Management Behavior Detection Platform Administration Guide* for information about user creation and providing access permission.

12. For Oracle Financial Services Regulatory Reporting (OFSRR) integration, you need to update the OFSRR web service end point URL after replacing actual value for the placeholders. To do so, follow these steps:

    Note: Placeholder variables are mentioned between double hashes (for example, `##PROTOCOL##`).

    a. Login to Alert Management Atomic Schema.

    b. Run the update query `"UPDATE KDD_INSTALL_PARAM SET ATTR_4_VALUE_TX='##PROTOCOL##://##RRSWEBSERVERIP##:##RRSWEBSERVERPORT##/##RRSAPPCONTEXT##/services/InitiateRequest' WHERE PARAM_ID=22"`

    c. Run the update query `"UPDATE KDD_INSTALL_PARAM SET ATTR_6_DESC_TX='##KEYPATH##'WHERE PARAM_ID=22`

Note: Update the placeholders ##PROTOCOL##, ##RRSWEBSERVERIP##,##RRSWEBSERVERPORT##,##RRSAPPCONTEXT## ,##KEYPATH## appropriately before running the query. ##KEYPATH## will be the path of `rrskey.des`, this file must have read, write, and execute permission to the application. This key file is available on OFSRR server.

CHAPTER 4

Setting up Oracle Financial Services Enterprise Case Management Analytic Reports and Threshold Analyzer

This chapter explains how to apply and display Analytic Reports and Threshold Analyzer in the OFS ECM UI.

This chapter includes the following topics:

- Installing OBIEE Server
- Post Installation Steps
- Deploying Analytic Reports

Installing OBIEE Server

To install Oracle Business Intelligence Enterprise Edition (OBIEE) server, refer to *Oracle® Business Intelligence Enterprise Edition Deployment Guide*,for more information.

Post Installation Steps

After installing the OBIEE server, follow these steps:

1. Run the update query in Alert Management Atomic Schema

   ```
   UPDATE KDD_INSTALL_PARAM SET
   ATTR_2_VALUE_TX='##PROTOCOL##://##OBIEESERVERIP##:##PORT_NUMBER
   ##' WHERE PARAM_ID=39
   ```

   ##OBIEESERVERIP##: is the IP address of the machine, where the OBIEE is installed.

   ##PORT_NUMBER##: is the port number used in OBIEE installation.

Example: If OBIEE is installed, then the machine IP address is 10.184.63.143, and the value of `Attr_2_value_tx for Param_id=39` is=http://10.184.63.143:9704.

Note: Port Number may change based on the OBIEE version. Give the Correct Port Number if it is not 9704.

Note: Verify the IP address of OFS ECM application URL in `Attr_4_value_tx for Param_id=39` in `Kdd_install_param` table. If the same OFS ECM application is deployed in different machine, then modify the IP address of OFS ECM Application URL in `Attr_4_value_tx for Param_id=39` in `Kdd_install_param` table appropriately.

Deploying Analytic Reports

To deploy Analytic Reports and Threshold Analyzer, follow these steps:

1. To stop Oracle Process Manager and Notification Server (OPMN) services, connect to the OBIEE installation server, and execute the following command.
   a. To do this go to: `<FMW_HOME>/instances/instance1/bin` directory and execute `./opmnctl stopall`

   Note: For Unix environment, execute the following command:

   b. To do this go to: `<FMW_HOME>/instances/instance1/bin` directory and execute `./opmnctl stopall`
2. Copy `Oracle_Mantas_6_BI0009` from

   `$FIC_HOME/OBIEE/repository` and place it under location `<FMW_HOME>/instance/instance1/bifoundation/OracleBIServerComponent/coreapplication_obis1/repository`
3. Search for string `[CACHE] in` the `NQSConfig.INI` file under: `<FMW_HOME>/instance/instance1/config/OracleBIServerComponent/coreapplication_obis1/NQSConfig.INI` location, and modify the default settings. The code should look similar to the following:

   ```
   From
   ENABLE = Yes;
   To
   ENABLE = No;
   ```

   If you are using OBIEE 11.1.1.6 or higher, then change the value in Nqsconfig.ini file located at `<FMW_HOME>/instances/instance1/config/OracleBIServerComponent/coreapplication_obis1/ directory`

   ```
   From
   EVALUATE_SUPPORT_LEVEL = 0;
   To
   EVALUATE_SUPPORT_LEVEL = 2;
   ```
4. Copy `ANALYTICS_REPORT` from `$FIC_WEB_HOME$/OBIEE /ANALYTICS_REPORT` and place under `<FMW_HoME>/instances/instance1/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/catalog`
5. Use below URL to log in to the Enterprise Manager: `(http://hostname:7001/em)` with User name: `Weblogic` and Password.

   Note: Password will be given at the time of installation.

6. Login to Enterprise Manager, click **Business Intelligence** and select Core Application.

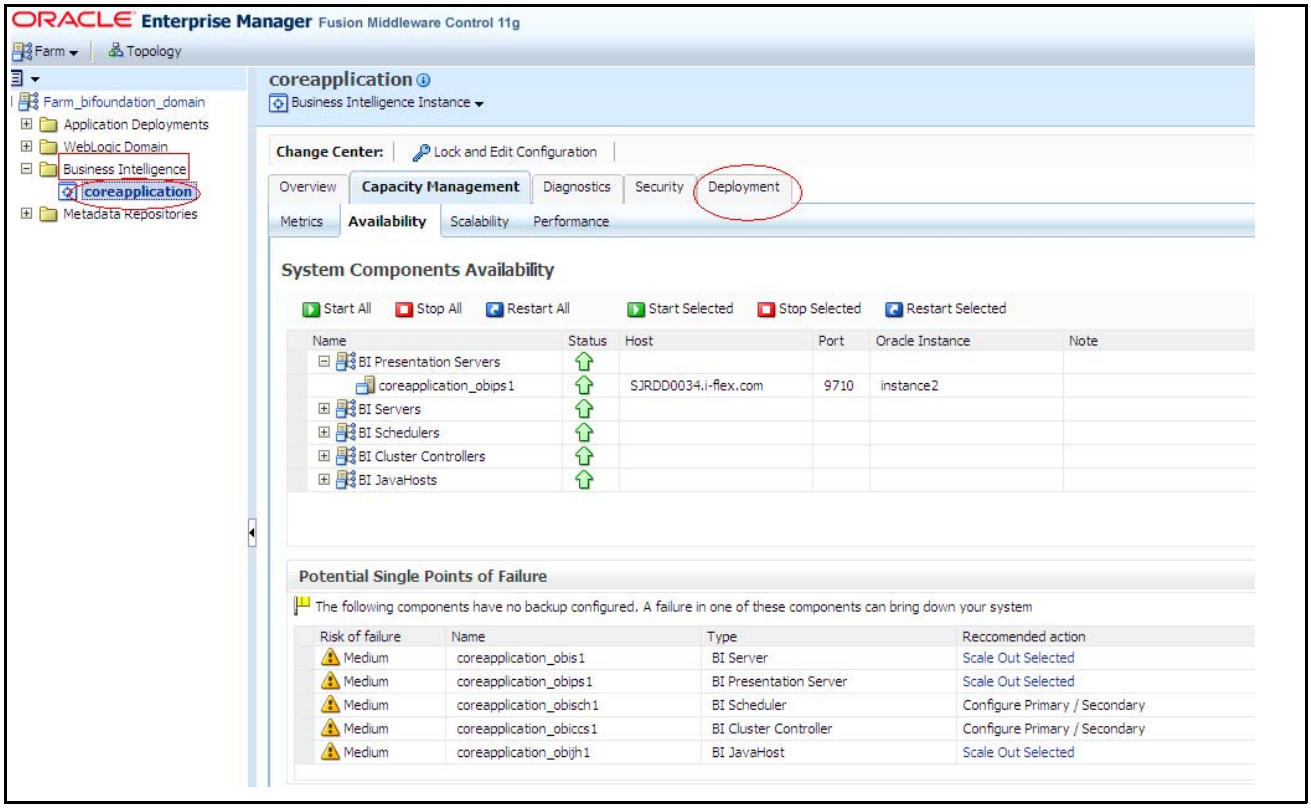

Figure 1. Business Intelligence Core Application page

7. Click **Deployment**. The Business Intelligence (BI) Server Repository page displays.

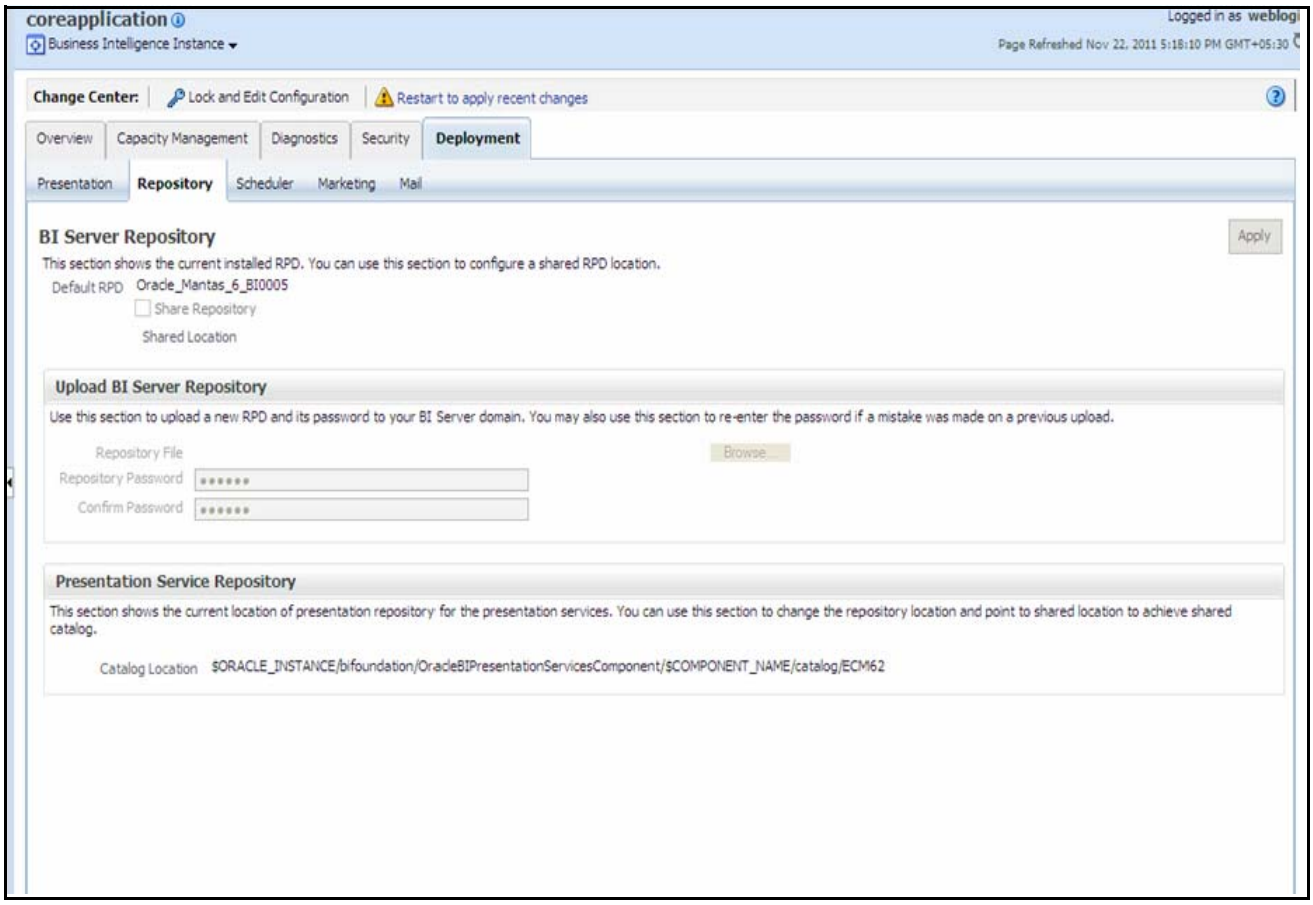

Figure 2. Application Lock and Edit Configuration page

8. Click **Repository** tab.
9. To update the Repository, click **Lock and Edit Configuration**.
10. In Upload BI Server Repository, browse the Repository file `<<FMW_HOME>instances/instance1/bifoundation/OracleBIServerComponent/coreapplication_obis1/repository/Oracle_Mantas_6_BI0009`
11. Enter Repository Password as `Mantas61`.
12. In Presentation Services Repository, give the Catalog Location as `<FMW_HOME>/instances/instance1/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/catalog/ANALYTICS_REPORT`
13. Click **Apply**, then click **Activate Changes**.
14. Copy `Page2.jsp` from `$FIC_WEB_HOME$/OBIEE/web` to `<FMW_HOME>/Oracle_BI1/bifoundation/web/app`

15. Modify the `Instanceconfig.xml` available at `<FMW_HOME>/Oracle_BI1/bifoundation/admin/config/OracleBIPresentationServicesComponent/instanceconfig.xml`. Paste the below code under:
"</ServerInstance> Tag

```
<Listener>
<Firewall>
<Allow address="127.0.0.1"/>
<Allow address="##OBIEE_INSTALLED_MACHINE_IP##"/>
</Firewall>
</Listener>
<Auth>
<SSO enabled="true">
<LogoffUrl>##PROTOCOL##://#WEB_SERVER_IP
#:#PORT#/analytics/saw.dll?Logoff</LogoffUrl>
<LogonUrl> ##PROTOCOL##://
WEB_SERVER_IP#:#PORT#/analytics/Page2.jsp</LogonUrl>
<ParamList>
<Param name="IMPERSONATE" source="httpHeader"
nameInSource="REMOTE_USER"/>
</ParamList>
</SSO>
</Auth>"
```

Note: Placeholders `OBIEE_INSTALLED_MACHINE_IP`, `WEB_SERVER_IP`, and `PORT` need to be replaced according to the deployed environment.

Note: If OBIEE installed machine IP is `10.184.62.165`, then above code must be as follows:

```
"<Listener>
<Firewall>
<Allow address="127.0.0.1"/>
<Allow address="10.184.62.165"/>
</Firewall>
</Listener>

<Auth>
<SSO enabled="true">

<LogoffUrl>http://10.184.62.165:9704/analytics/saw.dll?Logoff
</LogoffUrl>
<LogonUrl>
http://1.184.62.165:9704/analytics/Page2.jsp</LogonUrl>
<ParamList>
<Param name="IMPERSONATE" source="httpHeader"
nameInSource="REMOTE_USER"/>
</ParamList>
</SSO>
</Auth>"
```

16. Modify `Instanceconfig.xml` available at `<FMW_HOME>/instances/instance1/config/OracleBIPresentationServicesComponent/coreapplication_obips1/instanceconfig.xml` location

Note: If you are using OBIEE 11.1.1.5 or higher, then do not do step 16.

Add the tag (shown below) under the Security Section in `Instance Config.xml`

```
<InIFrameRenderingMode>allow</InIFrameRenderingMode>
<HardenXSS>false</HardenXSS>
```

Note: Refer below screen to add `IFrame` tag.

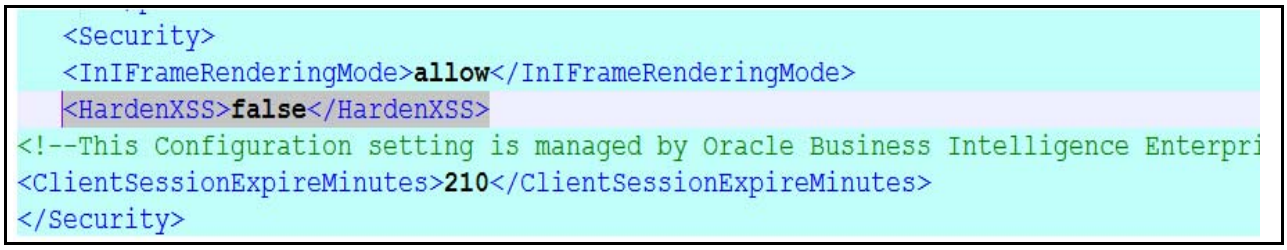

Figure 3. IFrame Tag Details

17. To start the OPMN services, connect to OBIEE Installation server, and execute the following command.

    a. To do this go to: `<FMW_HOME>/instances/instance1/bin` directory and execute the `./opmnctl startall`

    Note: For Unix environment, execute the following command:

    b. To do this go to: `<FMW_HOME>/instances/instance1/bin` directory and execute the `./opmnctl startall`

    Note: Refer to *Appendix A, About OBIEE* to update the connection pool in OBIEE.

CHAPTER 5

Deploying Network Visualization and Analysis

OFS ECM provides an enhanced network analysis utility, named Network Visualization and Analysis (also referred as NetViz). The NetViz generates networks based on the activity and entities involved in an alert or any entity in the research workflow. The Anti Money Laundering Solutions that use the Link Analysis algorithm, such as Networks of Accounts, Entities and Customers, and Hidden Relationships require the NetViz utility.

This chapter describes the process of deploying Network Visualization and Analysis utility to an existing Altio environment, assuming that Altio 5.1.5 and OFS ECM Active pages have been installed.

This chapter includes the following topics:

- Prerequisites
- Deploying Utility
- Removing Existing Installation
- Installing NetViz from New Installation Directory
- Configuring Network Visualization and Analysis

Prerequisites

The following prerequisites are required for deploying the Network Visualization and Analysis Utility:

- AltioLive 5.1.5 must be installed and configured (refer *Appendix B, Installing and Configuring Altio Server,* for more information).
- OFS ECM Active pages must be installed (refer *Appendix C, Installation of Oracle Financial Services Enterprise Case Management Active Pages,* for more information).

Deploying Utility

The Network Visualization and Analysis (NetViz) utility is packaged with the same directory structure that is used in the Altio environment, where the NetViz folders contain the required files for the corresponding folders in the Altio environment. Hence, the deployment task of copying files into appropriate directories and overwriting older versions are minimized.

The NetViz installation package contains the following directories:

- **Documentation**- This directory contains the associated documentation outlining, deploying, customizing, integrating, and using the NetViz.
- **New Installation**- This directory contains the files required to install NetViz to an environment, where it had never been installed.

Removing Existing Installation

If there is an existing installation of NetViz in Active Pages, delete the existing installation from AltioLive by following these steps:

1. After verifying whether the Altio Presentation Server is up and running, log in to the console `<Installation Server>:< Port>/<Altio Context>`.
2. Navigate to the Administration tab (for example, `username/pswd -admin/admin`).
3. Click **Sync Engine Admin Tool**.
4. Double-click the **Applications** folder.
5. Right-click **NETVIS** and select **Delete Application**.
6. Click **Save**.
7. Shut down the application server.
8. Change to `<AltioLive Root>/WEB-INF/classes/deploy` directory.
9. Delete the `netvis.aar.done` file.
10. Change to `<AltioLive Root>/WEB-INF/classes/apps` directory.
11. Delete NetViz folder.
12. Change to `<AltioLive Root>/WEB-INF/classes/backup` directory.
13. Delete all the contents of the directory.
14. Change to `<AltioLive Root>/WEB-INF/classes/preference` directory.
15. Delete all the contents of the directory.

Installing NetViz from New Installation Directory

To install NetViz from the `new_installation` directory, follow these steps:

1. Copy all the files from directory into `<AltioLive context root>`.
2. Start or restart the Web Application server to create a NetViz folder in the Apps directory.
3. Configure NetViz to work in your environment (Refer *Configuring Network Visualization and Analysis*, on page 31, for more information).
4. Start or restart if it is already running the Web Application server that hosts AltioLive
5. A server restart is required to reload server-side `jar` files and changes in internationalization to take effect.

Configuring Network Visualization and Analysis

Configuring Network Visualization and Analysis (NetViz) occurs at three levels:

1. Application Server level
2. Altio Presentation Server level
3. Network Manager Component level

The significance, mode, and values of the configuration process at each level is provided in the sections that follow:

Performing Application Server Configuration Tasks

Due to security constraints, all Web applications and associated servlets are required to be defined in the `web.xml`file, residing at `<AltioLive context root>\WEB-INF`. To meet this requirement, you must add the following servlet mapping to the `web.xml` file if it does not exist:

```
<servlet-mapping>
<servlet-name>MantasLogin</servlet-name>
<url-pattern>/netvis/*</url-pattern>
</servlet-mapping>
```

Note: Add the above servlet mapping if it does not exist, or if you are installing NetViz for the first time.

Performing Network Manager Component Configuration Tasks

The Network Manager (`networkmanager.jar`) is a server-side component that handles the retrieval and composition of networks from the database. It establishes a separate connection to a database using parameters supplied in the `hibernate.properties` file- (`<altiocontextroot>/WEB-INF/classes/hibernate.properties`).

The `hibernate.properties` file is a configuration file for the third-party software product Hibernate. This file is supplied in the NetViz bundle. However, you must ensure that the database URL, username, and password specified in this file are the same as those set as parameters in the Sync Engine Admin Tool.

Specify the values as follows:

- `hibernate.connection.username KDD_ALTIO`
- `hibernate.connection.password KDD_ALTIO`
- `hibernate.connection.url jdbc:oracle:thin:@demo3.mantas.com:1521:DEMO5`
- `hibernate.connection.driver_class oracle.jdbc.driver.OracleDriver`

Performing Altio Presentation Server Configuration Tasks

NetViz utilizes the server properties to establish a connection to the database and other required Oracle Financial Services applications. These server properties may have already been specified because they are shared across multiple applications. To complete the configuration of the Altio Presentation server, follow these steps:

1. Go to the following location: `<Altio Root>/WEB-INF/classes/apps/NetViz`
2. Edit `altioapp.xml`.
3. Go to the end of `altioapp.xml` file and replace `<PROPERTIES/>` tag with the following content:

```
 <PROPERTIES>

<PROPERTY NAME="mantas.db.driver" VALUE="<Java classpath for
database driver>"/>
<PROPERTY NAME="mantas.db.url" VALUE="<database URL>"/>
<PROPERTY NAME="mantas.db.user" VALUE="<database user name>"/>
<PROPERTY NAME="mantas.db.pwd" VALUE="<database user's
password>"/>
<PROPERTY NAME="mantas.domain.url" VALUE="<Business Data
Service URL>"/>
</PROPERTIES>
```

Replace the values of the parameters with the appropriate values for the database IP and its Username and Password. Refer to *Table 8 on page 33* for the default values.

Note: Business Data Service URL is the URL path of Oracle Financial Services 6.1 UI application. For example, `http://demo10.mantas.com:13080/MANTAS`

4. Click **Save**.
5. Restart the Altio 5.1.5 server.
6. To create Password property in an encrypted form, follow these steps:
   a. Login to the Altio Presentation Server Console.
   b. Navigate to the Tools tab.
   c. Specify the following:
      - Write Application ID: `netvis`
      - Username: `admin`
      - Password: `admin`
   d. Click **Application Manager**.
   e. Double-click the **Parameter** folder and select **`parameter - mantas.db.pwd`**. In Properties, select **`Y`** to encrypt.
   f. Click **Save**.

Note: After NetViz is configured at three levels, restart the server.

Table 8. Parameters for the Properties Tag in the altioapp.xml File

Property	Description	Default Value for NetViz
`mantas.db.url`	Database against which NetViz runs.	`jdbc:oracle:thin:@192.168.54.78:1521:DEMO5`
`mantas.db.driver`	Java classpath of the driver used to establish connections to the database.	`oracle.jdbc.OracleDriver`
`mantas.db.user`	A username to be used for the specified database.	`KDD_ALTIO`
`mantas.db.pwd`	The corresponding encrypted password for the supplied username.	`KDD_ALTIO` **Note:** The fields that require the encrypt property to be set as "Y" (Yes).

Configuring Websphere Server to Support the PNG MIME Type

To configure the Websphere server to support the PNG MIME type, and in order to run the NetViz without any error, follow these steps:

1. Login to the Websphere server Administrative Console.
2. Expand the Environments icon: forward arrow Virtual hosts.
3. Select **Default_host**.
4. Select **MIME Types** under Additional Properties.
5. Click **New**.
6. Enter `image/png` as the value for the MIME type field.
7. Enter `png` as the value for the Extension field.
8. Click **OK** to save the new MIME type.

Managing Cookies in WebLogic 10.3.1

WebLogic 10.3.1 and above default to tell the browser not to send any cookies back including `jsessionid` when requesting any scripting codes such as Javascripts and Java applets. This gives *You are no longer logged on* error message when logging into Altio.

To prevent this error, follow these steps:

1. Using a text editor, create an XML file and copy and paste the following:

```
<weblogic-web-app>
  <session-descriptor>
            <cookie-http-only>false</cookie-http-only>
  </session-descriptor>
  <container-descriptor>
  <!-- fix the classloader order so JDOM and Axis work.  -->
<!-- see http://ws.apache.org/axis/java/install.html#WebLogic8.1 -->
       <prefer-web-inf-classes>true</prefer-web-inf-classes>
  </container-descriptor>
</weblogic-web-app>
```

2. Name the file `weblogic.xml` and save it.
3. Place the `weblogic.xml` file under the Altio's and OFSAAI web application's WEB-INF folder.
4. Restart the server.

Configuring WebLogic Application Server to support the PNG MIME type

To configure WebLogic Application Server to support the PNG MIME type in order to run NetViz without any error, follow these steps:

1. Create a new file, named `mimemappings.properties` in the domain directory containing the Oracle Financial Services application.

   Paste the following contents in the file:

   ```
   bmp=image/bmp
   gif=image/gif
   JPE=image/jpeg
   JPEG=image/jpeg
   JPG=image/jpeg
   jpe=image/jpeg
   jpeg=image/jpeg
   jpe=image/jpeg
   png=image/png
   PNG=image/png
   ```

2. Save the file.
3. Restart the WebLogic Application server.

APPENDIX A

About OBIEE

This appendix outlines the steps required to configure Oracle Financial Services Business Intelligence Enterprise Edition.

This appendix includes the following topics:

- Creating ODBC Connection
- Configuring OBIEE Connection Pool
- Configuring OBIEE Dashboard Access Control

Creating ODBC Connection

To connect to OBIEE from your local machine, you must create an ODBC connection. To create an ODBC connection, follow these steps:

1. Click **Start**, and select **Run**.

   The Run dialog box displays.

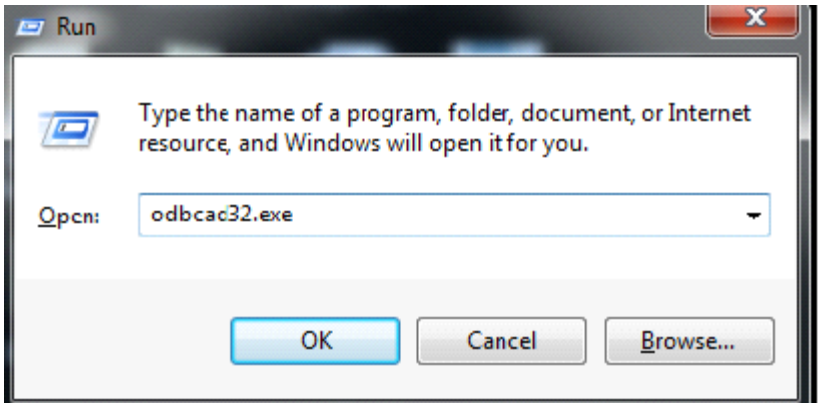

Figure 4. Run Dialog Box

2. Enter `odbcac32.exe` in the Open field and click **OK**.

   The ODBC Data Source Administer dialog box displays.

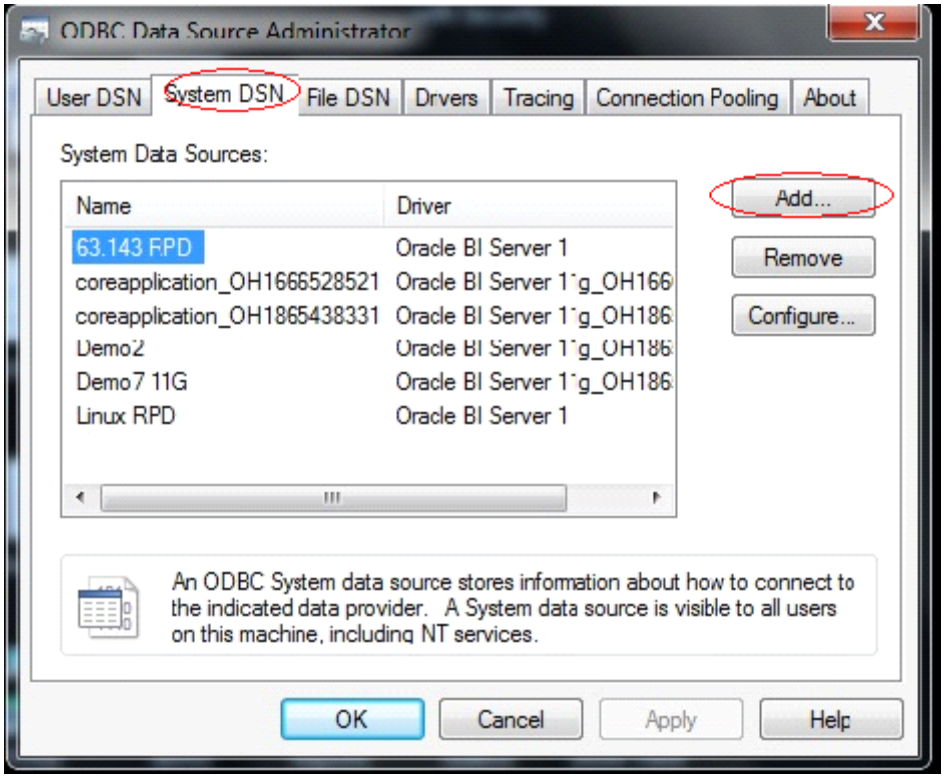

Figure 5. ODBC Data Source Administrator Dialog Box

3. Select System DSN tab and click **Add**.

   The Create New Data Source dialog box displays.

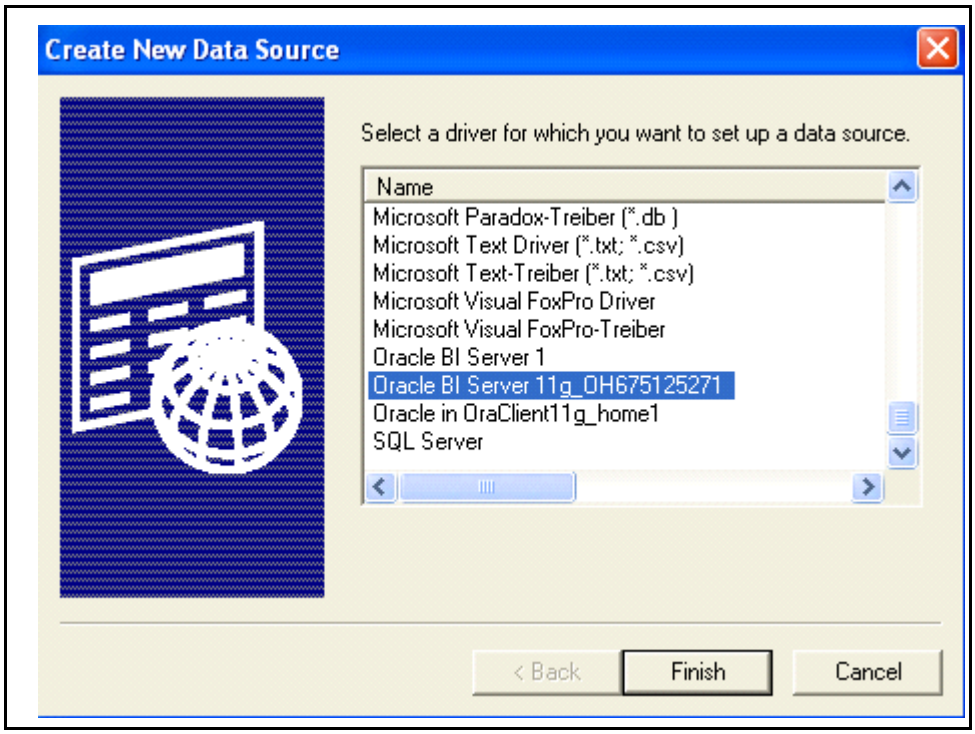

Figure 6. Create New Data Source Dialog Box

4. Select the correct driver, for example "`Oracle BI Server 11g_xxxxxx`" as a driver and click **Finish**.

   The Oracle BI Server DSN Configuration dialog box displays.

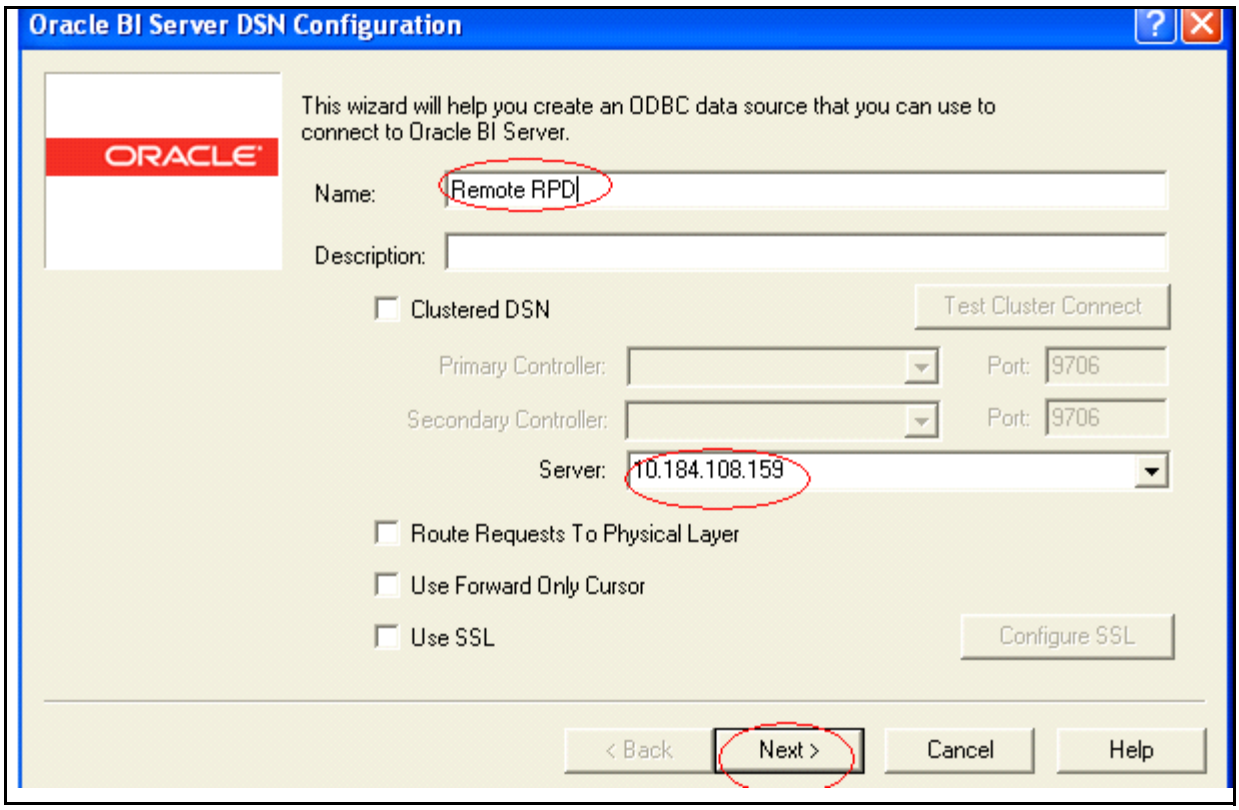

Figure 7. Oracle BI Server DSN Configuration Dialog Box

5. Enter the name in the Name field and IP address of OBIEE server in Server field. Click **Next**.

   The Oracle BI Server DSN Configuration Login dialog box displays.

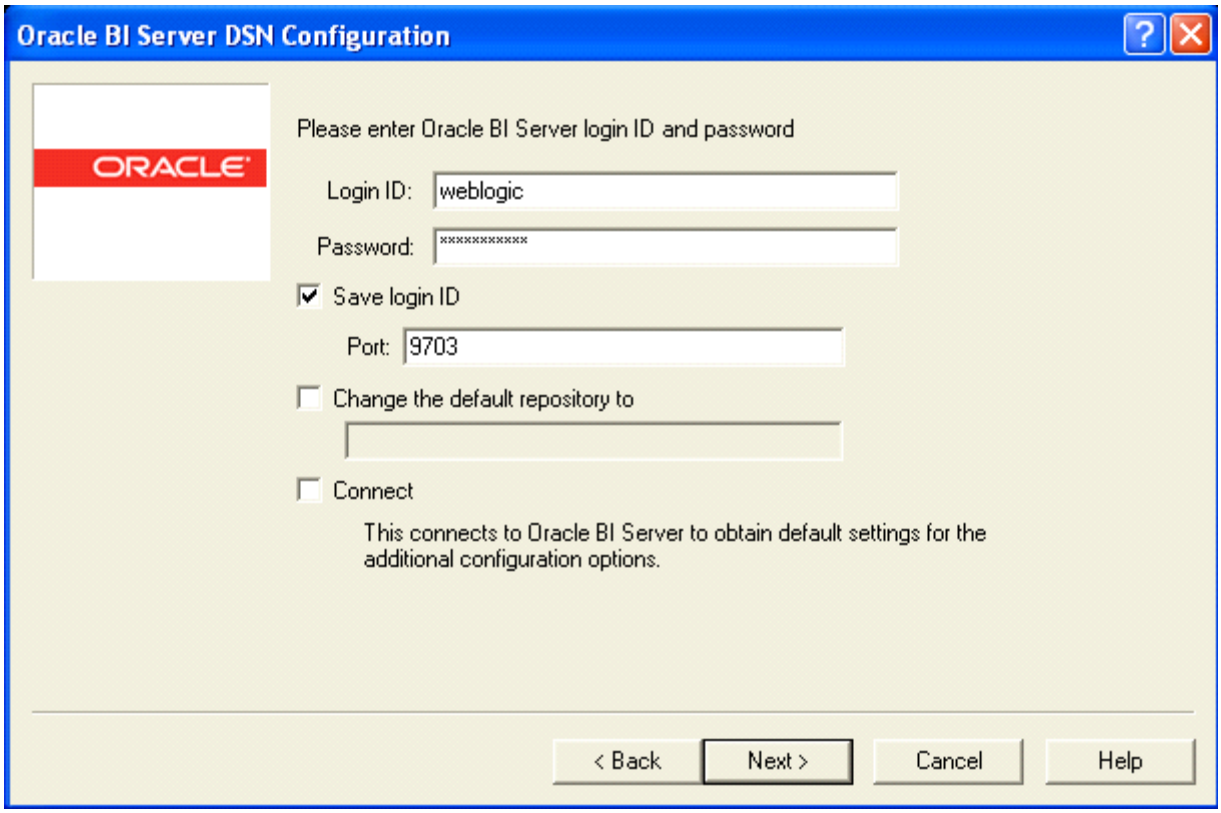

Figure 8. Oracle BI Server DSN Configuration Login Dialog Box

6. Enter Login ID as `weblogic` and Password.
   Note: The user password will be given at the time of installation.
7. Click **Next**.
8. Click **Finish**.

Configuring OBIEE Connection Pool

1. Click **Start**, point to **Programs** , then click **Oracle Business Intelligence** option, and then click **Administration**. The Oracle BI Administration Tool page displays.

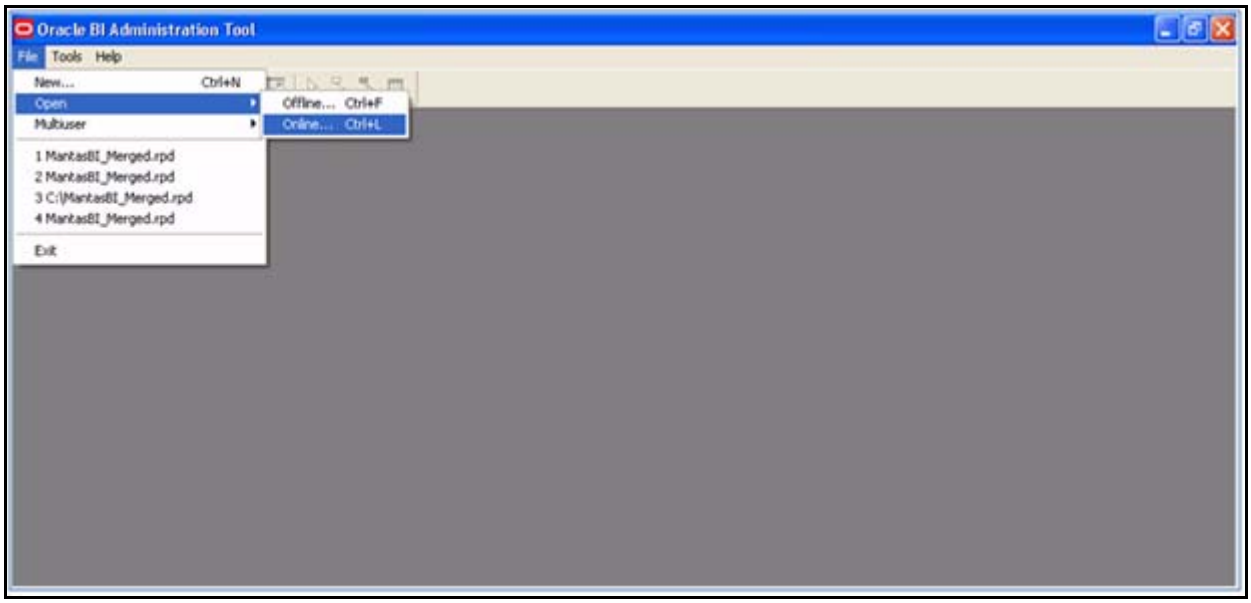

Figure 9. Oracle BI Administration Tool

2. From the File menu, select **Open** and click **Online**.

   The Open Online `<database name>` dialog box displays.

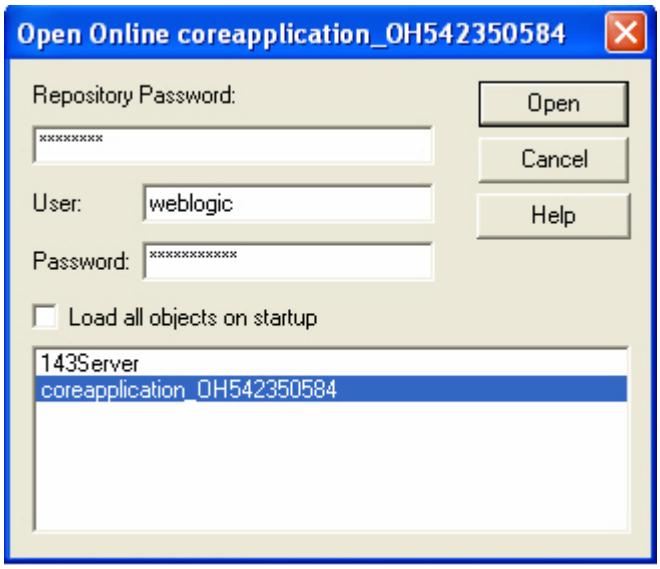

Figure 10. Open Online Dialog Box

3. Select the ODBC name.
4. Enter the User as `Weblogic` and Password.

   Note: The User Password will be given at the time of installation. Repository Password is `Mantas61`
5. Click **Open**.

   The Oracle BI Administration Tool - `Oracle_Mantas_6_BI0009.rpd` windows displays.

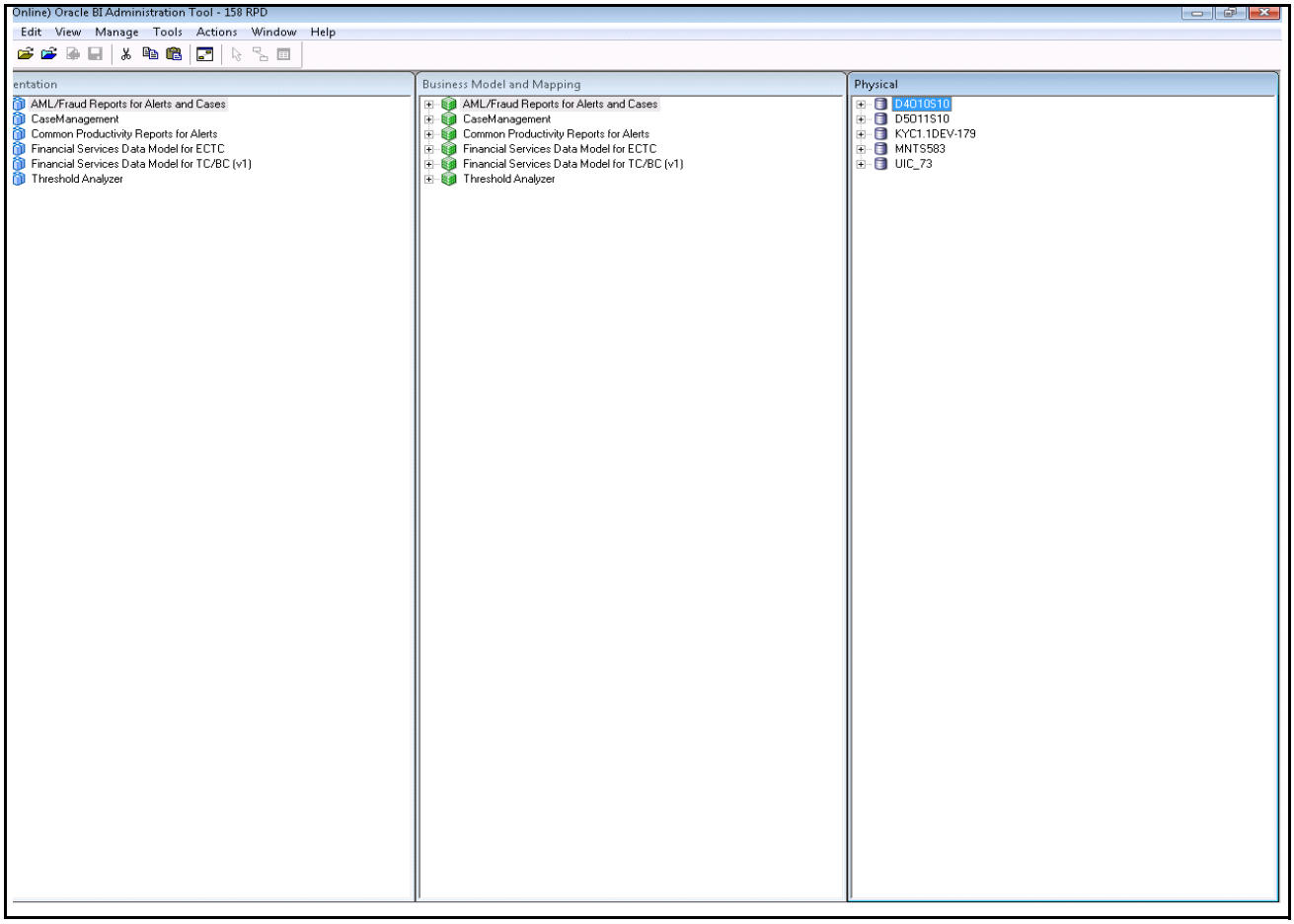

Figure 11. Oracle BI Administration Tool - MantasBI_Merged.rpd

6. In the Physical section, under the database name, double-click **Connection Pool** to open the Connection Pool Properties dialog box.

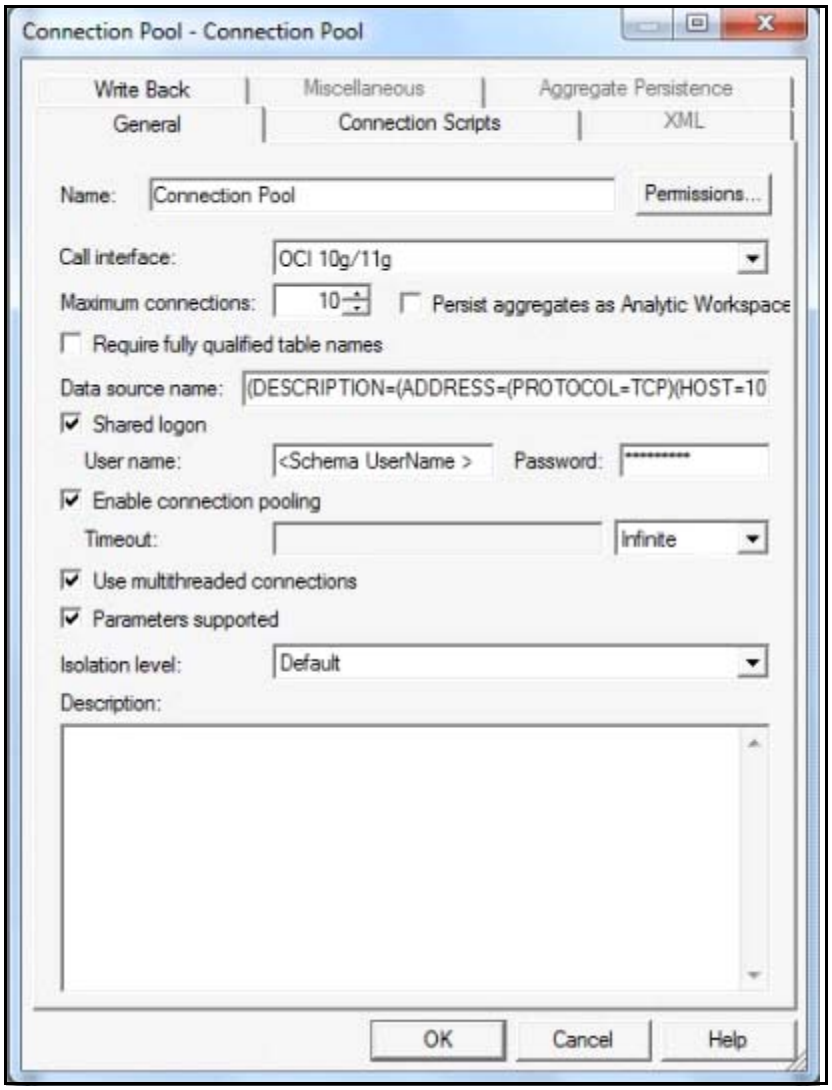

Figure 12. Connection Pool Dialog Box

7. In the Connection Pool dialog box, follow these steps:
   a. Select the **General** tab.
   b. Enter Data Source Name `(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<Database IP>)(PORT=<port no>))(CONNECT_DATA=(SID=<Instance Name>)))` in the Data Source Name text field.
   c. Enter the relevant User name and Password for schema.
   d. Click **OK** and **Save**.

   Note: Similarly change the Connection Pools in Physical Layer based on which the database you are connecting.

Schema details for all Connection Pools:

- `D4010S10->Alert Management Schema`
- `D5011S10->Report Schema`
- `KYC1.1DEV-179->Alert Management Schema`
- `MNTS583->Report Schema`
- `UIC_73->Case Management Schema`
- `UIC_73-> Security connection pool->Alert Management Schema`

Configuring OBIEE Dashboard Access Control

To implement this step, you must create AUTH group in OFS ECM application. Assign a user to AUTH group in OFS ECM application. That means security view in Mantas Schema user group column must contain AUTH group.

1. Access the application using the following URL:
   `https://<server>:<port>/analytics`

Figure 13. Oracle Business Intelligence Login Page

2. Enter the User ID (users ID must belongs to AUTH group) and Password, and then click **Sign In**.

   The OBIEE Dashboard page displays.

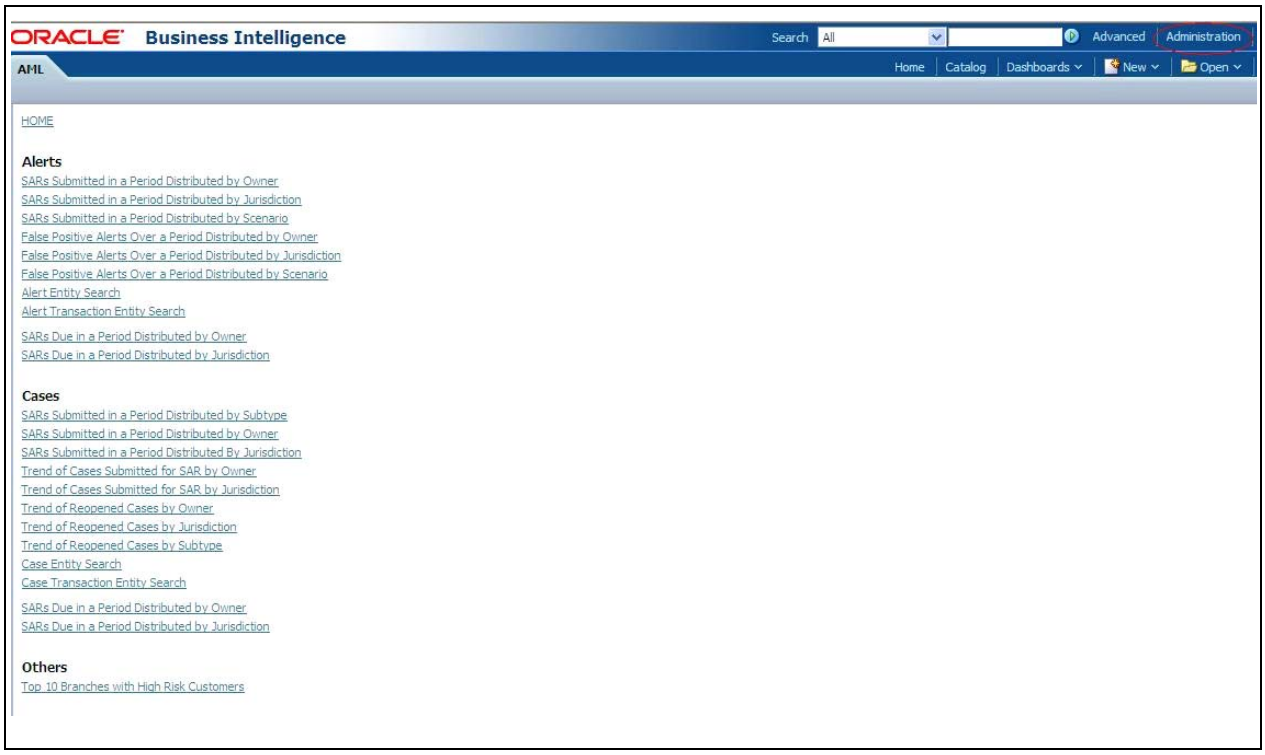

Figure 14. OBIEE Dashboard Page

3. Check the Security view in Mantas Schema. Find out the users and groups in Security view. It is based on what you need to assign to a user groups in Manage Presentation Catalog groups in OBIEE.
4. Click **Administration**.

   The Manage Catalog Group page displays.

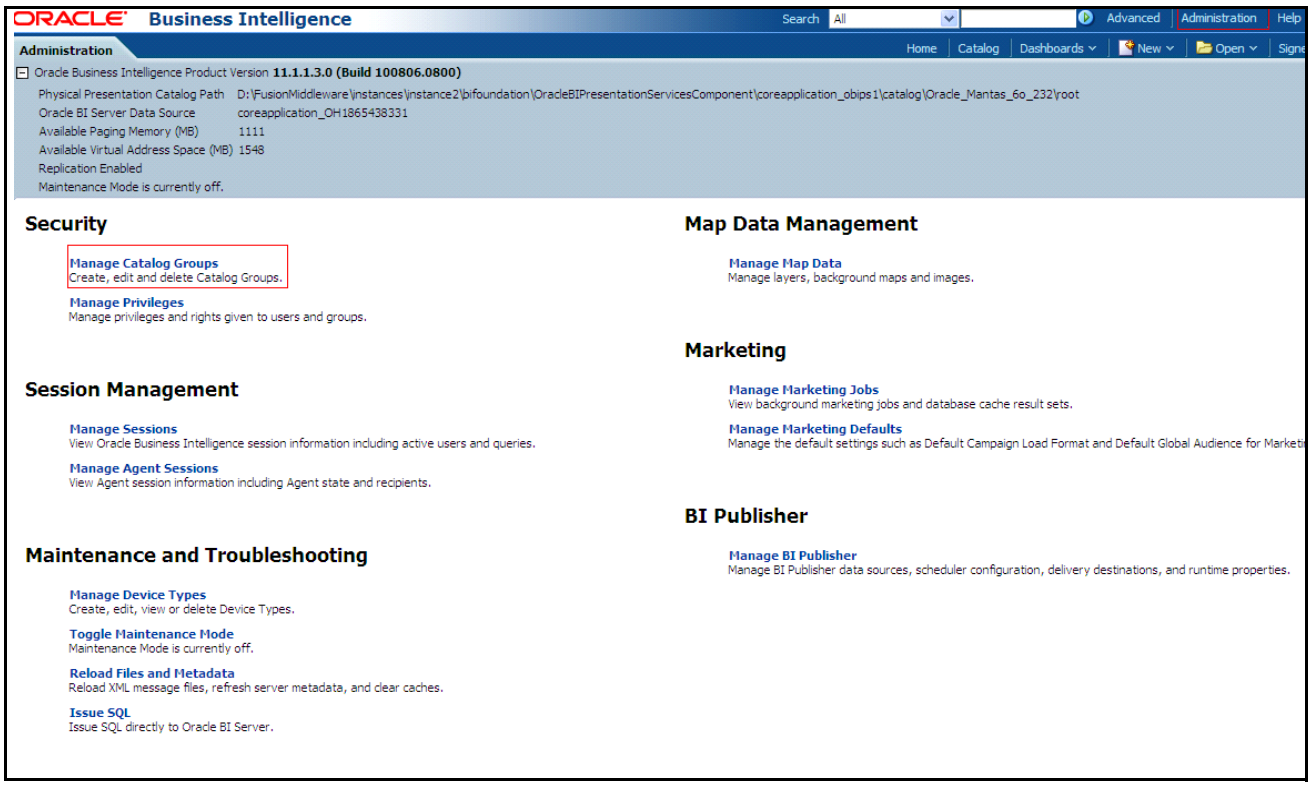

Figure 15. Manage Catalog Group page

5. In Security, click **Manage Catalog Group** link. The Manage Catalog Group page displays.

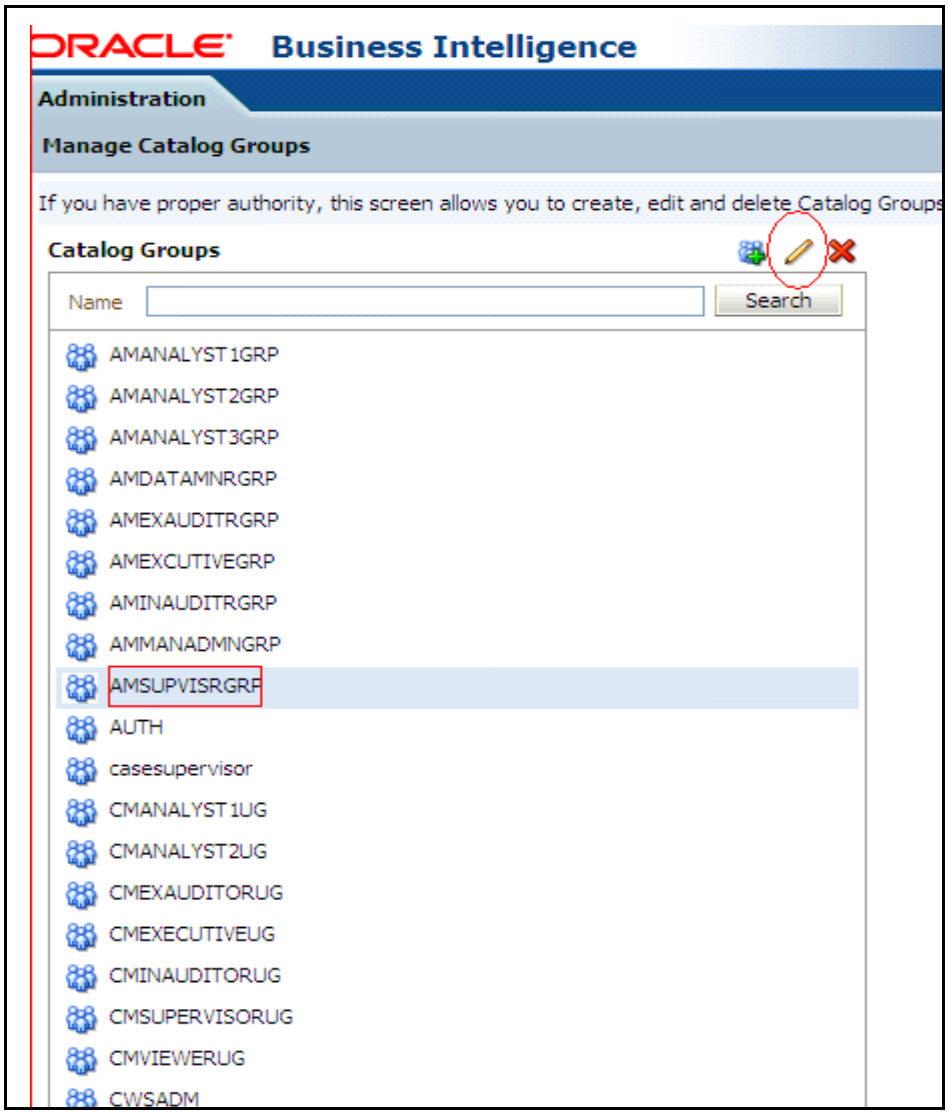

Figure 16. Manage Catalog Group Names page

6. Select the particular catalog group and click Edit sign. The Edit Group page displays. This page gives you a complete details of the selected Catalog Group.

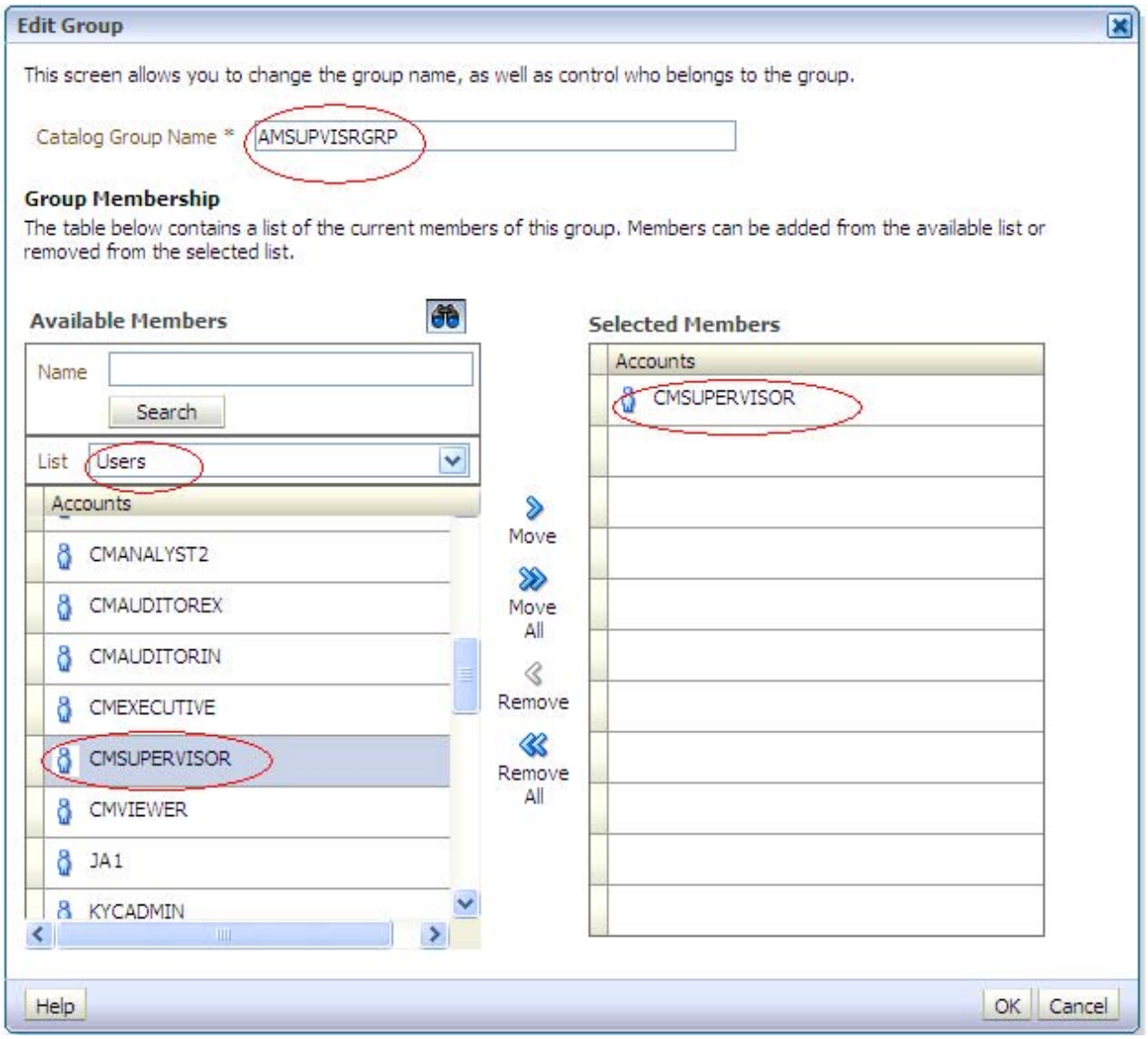

Figure 17. Edit Group page

7. Select the Users option from the drop-down list. From the Users list, select the relevant user to assign a group and click **Move** to move the selected user to the Selected Members Account column.

   Note: If the Administrator is unable to see any users in the Available Members list, then those particular missing users need to acknowledge their account by logging into OFS ECM application.

8. Click **OK**.

   Note: check whether the user is already mapped to a Catalog Group or not. If the user is already mapped then no need to perform above steps.

APPENDIX B

Installing and Configuring Altio Server

This appendix outlines the steps required to install the Altio Presentation Server.

This appendix includes the following topics:

- Installing Altio Presentation Server
- Accessing Altio Presentation Server Console
- Configuring Altio Presentation Server

Installing Altio Presentation Server

1. Identify the following details before installing the Altio Presentation Server:
   - Host machine on which the Altio Presentation Server is to reside. For example, `xxxhost.domain.com`
   - Web Application server on which the Altio Presentation Server is to deploy.
   - Port of Web Application Server from which the Altio Presentation Server is to be connected. For example, `xxxhost.domain.com:7001`, where `7001` is the port number.

   Note: You are allowed to deploy the Altio Presentation Server either on the same Web Application server instance where the OFS ECM UI is installed, or on a dedicated Web Application server instance.
   - The Altio context-root is used to access the Altio Presentation Server. For example, `http://xxxhost.domain.com:7001/altio51`, where `altio51` is the context-root.
2. Install the recommended version of the Altio Presentation Server on a Web Application server using the parameters identified above.

   Note: Refer to the *Altio Deployment Guide* for installing the Altio Presentation Server. You must provide an Altio license file during the Altio installation process. Contact FCCM Customer Support for a license file for Altio Presentation Server at licensecodes_ww@oracle.com.

Note: By default, the installer updates the `kdd_install_param` table of Alert Management atomic schema for altio context as `altio51`. If the context deployed on a Web Application server is different, then follow the these steps:

a. Login to Alert Management Atomic schema.

b. Execute the following update query:

```
UPDATE KDD_INSTALL_PARAM SET
ATTR_1_VALUE_TX='<<NEW_ALTIO_CONTEXT>>'WHERE PARAM_ID=21;
```

Note: Replace the placeholder `<<NEW_ALTIO_CONTEXT>>` with the deployed Altio context name.

3. In case Altio application is deployed on a different machine than the Web layer installed machine, follow these steps:

a. Login to Alert Management Atomic Schema.

b. Run the update query after replacing the placeholders `##PROTOCOL##,##ALTIO_DEPLOYED_MACHINE_IP_ADDRESS##,##PORTNO##` appropriately.

c.
```
UPDATE KDD_INSTALL_PARAM SET
ATTR_2_VALUE_TX='##PROTOCOL##://##ALTIO_DEPLOYED_MACHINE_IP_
ADDRESS##:##PORTNO##' WHERE PARAM_ID=21
```

Note:

- `##PROTOCOL##` is web page access protocol (http or https)
- `##ALTIO_DEPLOYED_MACHINE_IP_ADDRESS##` is altio deployed web server IP Address
- `##PORTNO##` is the port number of the web server port number

d. Commit the Database changes

Accessing Altio Presentation Server Console

After installing the Altio Presentation Server, open the following URL from the recommended Web browser: `http://<host>:<port>/<context-root>`. The Altio Console front page displays.

Note: Refer to *Table 2 Environment Details,* on page 1, for the recommended Web browsers. Refer to the *Altio User Guide -How to log in to the Altio Console* section, for more information.

Configuring Altio Presentation Server

To configure the Altio Presentation Server, follow these steps:

1. Modify the following in `web.xml file`.

```
From:
<servlet-mapping>
<servlet-name>AltioLogin</servlet-name>
<url-pattern>/login/*</url-pattern>
</servlet-mapping>
To:
<servlet-mapping>
<servlet-name>MantasLogin</servlet-name>
<url-pattern>/login/*</url-pattern>
</servlet-mapping>
```

2. Add the following content to the `web.xml` file.

```
<servlet>
<servlet-name>MantasLogin</servlet-name>
<servlet-class>MantasAPLoginHandler</servlet-class>
</servlet>
```

3. If you are deploying Network Visualization (NetViz), add the following content to the `web.xml` file:

```
<servlet-mapping>
<servlet-name>MantasLogin</servlet-name>
<url-pattern>/netvis/*</url-pattern>
</servlet-mapping>
```

Note: The `web.xml` file is located at following locations:

- **WebLogic**:`<altio_directory>/WEB_INF/web.xml`
- **Tomcat:** `<altio_directory>/WEB_INF/web.xml`

4. Delete the default content inside the following directories.
   - `<altio_deployed_directory>/WEB-INF/classes/backup`
   - `<altio_deployed_directory>/WEB-INF/classes/preference`
5. Restart the Altio Presentation Server to make the changes take effect.

Note: Additional step for WebLogic:

6. Modify the following in the `<altio_deployed_directory>/WEB_INF/classes/conf/altioserver.xml` file:

```
From:
<INIT> ... <ACCEPTENCODING VALUE="x-altio-ser,gzip,compress"/>
To:
<INIT> ... <ACCEPTENCODING VALUE="x-altio-ser"/>
```

APPENDIX C

Installation of Oracle Financial Services Enterprise Case Management Active Pages

This appendix outlines the steps required to extract Oracle Financial Services Active Pages from the Active Pages installer package.

Extracting Oracle Financial Services Active Pages

To extract Oracle Financial Services Active Pages from the Active Pages installer package, follow these steps:

1. Extract the following files from the media pack to a working directory on the host where the Web Application server is running:
   - `install.sh`
   - `MantasAP.tar`
2. Ensure that the `install.sh` script has execute rights. If the script does not have the execute rights, then run the following command:

   ```
   chmod 550 install.sh
   ```
3. Stop the Web Application server that is running the Altio Presentation Server.
4. Run the `install.sh` script from the directory where you have saved the `MantasAP.tar file`. The calling syntax is: `install.sh <ORACLE_HOME> <ORACLE_VERSION> <altio_deployed_directory>[license-file]`

   Note: The only optional parameter is license-file. If omitted, the Altio Presentation Server uses the license file provided during Altio Presentation Server installation, which is available under `<altio_deployed_directory>/WEB_INF/classes/conf/altiolicence.xml`